



CVE-2014-1893

Published on: 03/31/2014 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:25:47 PM UTC

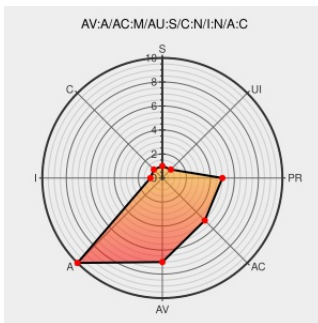
CVE-2014-1893

[Source: Mitre](#)

[Source: NIST](#)

[CVE.ORG](#)

[Print: PDF](#)



Certain versions of [Xen](#) from [Xen](#) contain the following vulnerability:

Multiple integer overflows in the (1) FLASK_GETBOOL and (2) FLASK_SETBOOL suboperations in the flask hypercall in Xen 4.1.x, 3.3.x, 3.2.x, and earlier, when XSM is enabled, allow local users to cause a denial of service (processor fault) via unspecified vectors, a different vulnerability than CVE-2014-1891, CVE-2014-1892, and CVE-2014-1894.

CVE-2014-1893 has been assigned by [M](#) cve@mitre.org to track the vulnerability

CVSS2 Score: **5.2 - MEDIUM**

**Access
Vector**

ADJACENT_NETWORK

**Access
Complexity**

MEDIUM

Authentication

SINGLE

**Confidentiality
Impact**

NONE

**Integrity
Impact**

NONE

**Availability
Impact**

COMPLETE

CVE References

Description

Tags

Link

oss-security - Re: Xen Security Advisory 84 - integer overflow in several XSM/Flask hypercalls

[www.openwall.com
text/html](http://www.openwall.com/text/html)

[MLIST \[oss-security\] 20140207 Re: Xen Security Advisory 84 - integer overflow in several XSM/Flask hypercalls](#)

[security-announce] SUSE-SU-2014:0373-1: important: Security update for

[lists.opensuse.org
text/html](https://lists.opensuse.org/text/html)

[SUSE SUSE-SU-2014:0373](#)

XSA-84 - Xen Security Advisories

[Patch](#)
[Vendor Advisory](#)
xenbits.xen.org
[text/html](#)

[CONFIRM xenbits.xen.org/xsa/advisory-84.html](#)

oss-security - Xen Security Advisory 84 (CVE-2014-1891,CVE-2014-1892,CVE-2014-1893,CVE-2014-1894) - integer overflow in several XSM/Flask hypercalls

[www.openwall.com
text/html](http://www.openwall.com/text/html)

[MLIST \[oss-security\] 20140210 Xen Security Advisory 84 \(CVE-2014-1891,CVE-2014-1892,CVE-2014-1893,CVE-2014-1894\) - integer overflow in](#)

oss-security - Re: Xen Security Advisory 84 - integer overflow in several XSM/Flask hypercalls

[www.openwall.com
text/html](http://www.openwall.com/text/html)

 [MLIST \[oss-security\] 20140207 Re: Xen Security Advisory 84 - integer overflow in several XSM/Flask hypercalls](#)

Gentoo Linux Documentation -- Xen: Multiple Vulnerabilities

[security.gentoo.org
text/html](http://security.gentoo.org/text/html)

 [GENTOO GLSA-201407-03](#)

[security-announce] SUSE-SU-2014:0446-1: important: Security update for

[lists.opensuse.org
text/html](http://lists.opensuse.org/text/html)

 [SUSE SUSE-SU-2014:0446](#)

[security-announce] SUSE-SU-2014:0372-1: important: Security update for

[lists.opensuse.org
text/html](http://lists.opensuse.org/text/html)

 [SUSE SUSE-SU-2014:0372](#)

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Xen	Xen	3.2.0	All	All	All
Operating System	Xen	Xen	3.2.1	All	All	All
Operating System	Xen	Xen	3.2.2	All	All	All
Operating System	Xen	Xen	3.2.3	All	All	All
Operating System	Xen	Xen	3.3.0	All	All	All
Operating System	Xen	Xen	3.3.1	All	All	All
Operating System	Xen	Xen	3.3.2	All	All	All
Operating System	Xen	Xen	3.4.0	All	All	All
Operating System	Xen	Xen	3.4.1	All	All	All
Operating System	Xen	Xen	3.4.2	All	All	All
Operating System	Xen	Xen	3.4.3	All	All	All
Operating System	Xen	Xen	3.4.4	All	All	All
Operating System	Xen	Xen	4.0.0	All	All	All

Operating System	Xen	Xen	4.0.1	All	All	All
Operating System	Xen	Xen	4.0.2	All	All	All
Operating System	Xen	Xen	4.0.3	All	All	All
Operating System	Xen	Xen	4.0.4	All	All	All
Operating System	Xen	Xen	4.1.0	All	All	All
Operating System	Xen	Xen	4.1.1	All	All	All
Operating System	Xen	Xen	4.1.2	All	All	All
Operating System	Xen	Xen	4.1.3	All	All	All
Operating System	Xen	Xen	4.1.4	All	All	All
Operating System	Xen	Xen	4.1.5	All	All	All
Operating System	Xen	Xen	3.2.0	All	All	All
Operating System	Xen	Xen	3.2.1	All	All	All
Operating System	Xen	Xen	3.2.2	All	All	All
Operating System	Xen	Xen	3.2.3	All	All	All
Operating System	Xen	Xen	3.3.0	All	All	All
Operating System	Xen	Xen	3.3.1	All	All	All
Operating System	Xen	Xen	3.3.2	All	All	All
Operating System	Xen	Xen	3.4.0	All	All	All
Operating System	Xen	Xen	3.4.1	All	All	All
Operating System	Xen	Xen	3.4.2	All	All	All
Operating System	Xen	Xen	3.4.3	All	All	All
Operating System	Xen	Xen	3.4.4	All	All	All
Operating System	Xen	Xen	4.0.0	All	All	All

Operating System	Xen	Xen	4.0.1	All	All	All
Operating System	Xen	Xen	4.0.2	All	All	All
Operating System	Xen	Xen	4.0.3	All	All	All
Operating System	Xen	Xen	4.0.4	All	All	All
Operating System	Xen	Xen	4.1.0	All	All	All
Operating System	Xen	Xen	4.1.1	All	All	All
Operating System	Xen	Xen	4.1.2	All	All	All
Operating System	Xen	Xen	4.1.3	All	All	All
Operating System	Xen	Xen	4.1.4	All	All	All
Operating System	Xen	Xen	4.1.5	All	All	All
Operating System	Xen	Xen	All	All	All	All
cpe:2.3:o:xen:xen:3.2.0:*****:						
cpe:2.3:o:xen:xen:3.2.1:*****:						
cpe:2.3:o:xen:xen:3.2.2:*****:						
cpe:2.3:o:xen:xen:3.2.3:*****:						
cpe:2.3:o:xen:xen:3.3.0:*****:						
cpe:2.3:o:xen:xen:3.3.1:*****:						
cpe:2.3:o:xen:xen:3.3.2:*****:						
cpe:2.3:o:xen:xen:3.4.0:*****:						
cpe:2.3:o:xen:xen:3.4.1:*****:						
cpe:2.3:o:xen:xen:3.4.2:*****:						
cpe:2.3:o:xen:xen:3.4.3:*****:						
cpe:2.3:o:xen:xen:3.4.4:*****:						
cpe:2.3:o:xen:xen:4.0.0:*****:						
cpe:2.3:o:xen:xen:4.0.1:*****:						
cpe:2.3:o:xen:xen:4.0.2:*****:						

cpe:2.3:o:xen:xen:4.0.3:*****:
cpe:2.3:o:xen:xen:4.0.4:*****:
cpe:2.3:o:xen:xen:4.1.0:*****:
cpe:2.3:o:xen:xen:4.1.1:*****:
cpe:2.3:o:xen:xen:4.1.2:*****:
cpe:2.3:o:xen:xen:4.1.3:*****:
cpe:2.3:o:xen:xen:4.1.4:*****:
cpe:2.3:o:xen:xen:4.1.5:*****:
cpe:2.3:o:xen:xen:3.2.0:*****:
cpe:2.3:o:xen:xen:3.2.1:*****:
cpe:2.3:o:xen:xen:3.2.2:*****:
cpe:2.3:o:xen:xen:3.2.3:*****:
cpe:2.3:o:xen:xen:3.3.0:*****:
cpe:2.3:o:xen:xen:3.3.1:*****:
cpe:2.3:o:xen:xen:3.3.2:*****:
cpe:2.3:o:xen:xen:3.4.0:*****:
cpe:2.3:o:xen:xen:3.4.1:*****:
cpe:2.3:o:xen:xen:3.4.2:*****:
cpe:2.3:o:xen:xen:3.4.3:*****:
cpe:2.3:o:xen:xen:3.4.4:*****:
cpe:2.3:o:xen:xen:4.0.0:*****:
cpe:2.3:o:xen:xen:4.0.1:*****:
cpe:2.3:o:xen:xen:4.0.2:*****:
cpe:2.3:o:xen:xen:4.0.3:*****:
cpe:2.3:o:xen:xen:4.0.4:*****:
cpe:2.3:o:xen:xen:4.1.0:*****:
cpe:2.3:o:xen:xen:4.1.1:*****:
cpe:2.3:o:xen:xen:4.1.2:*****:

cpe:2.3:o:xen:xen:4.1.3:*****:
cpe:2.3:o:xen:xen:4.1.4:*****:
cpe:2.3:o:xen:xen:4.1.5:*****:
cpe:2.3:o:xen:xen:*****:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→